MAR 2 7 2007
PATENT & TRADEMARK OFFICE

Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. (Currently Amended) A method of addressing data errors in a computer system, comprising:

pre-determining a software-programmable data poisoning policy to control actions to be taken based on different classes of data poisoning events;

error-checking a unit of data;

detecting an uncorrectable error in the unit of data;

if ~~at least one~~ the uncorrectable error is detected in the unit of data, based on the pre-determined data poisoning policy, determining if the ~~at least one~~ detected uncorrectable error is a data poisoning event;

~~and if so,~~ marking the unit of data containing ~~with an indication that the unit of data contains~~ a data poisoning event with a software-visible bit;

determining, based on [[a]] the pre-determined data poisoning policy, if the unit of data containing the poisoning event is to be acted upon~~, and if so, detecting, by the computer system, the presence of the indication that the unit of data contains a data poisoning event~~;

detecting by an operating system the software-visible bit in the data unit; and

in accordance with the detected software-visible control bit and the pre-determined data poisoning policy, acting, by [[an]] the operating system of the computer system, ~~upon the presence of the indication~~ to address the presence of ~~erroneous~~ the uncorrectable error ~~data~~ in the unit of data, wherein the operating system is not always brought down ~~upon the presence of the indication~~.

2. (Currently Amended) The method of Claim 1, wherein [[said]] error-checking comprises:

applying error-control decoding to the unit of data.

3. (Currently Amended) The method of Claim 2, wherein [[said]] error-checking further comprises:

correcting [[any]] correctable errors in the unit of data.

4. (Cancelled).

5. (Currently Amended) The method of Claim 1, wherein [[said]] acting to address ~~upon~~ the presence of the ~~indication~~ uncorrectable error comprises:

removing the unit of data including the uncorrectable error from use by the operating system.

6. (Currently Amended) The method of Claim 5, ~~wherein said acting upon the presence of the indication~~ further comprising ~~comprises~~:

recovering the unit of data.

7. (Cancelled).

8. (Currently Amended) The method of Claim 1, further comprising:

if the operating system detects the software-visible bit, ~~the presence of said indication that the unit of data contains a data poisoning event,~~ determining if the unit of data is in user space; and

if the unit of data is in user space, terminating an application running on the computer system and removing the unit of data from use by the operating system.

9. (Original) The method of Claim 1, further comprising:

upon detection of an uncorrectable error in said unit of data, providing information to said operating system to enable recovery of said unit of data.

10. (Original) The method of Claim 9, wherein the information includes a target address corresponding to said unit of data.

11-12. (Cancelled).

13. (Currently Amended) The method of Claim 1, wherein [[said]] detecting is performed by at least one of ~~unit selected from the group consisting of:~~ a processor [[and]] or a memory.

14. (Currently Amended) A computer system comprising:

a software-programmable data poisoning policy to control actions to be taken based on different classes of data poisoning events;

~~at least one~~ a processor;

at least one error control decoding implementation including at least one ~~selected from the group consisting~~ of an error-control decoder, a software to implement error-control decoding by the ~~at least one~~ processor, or a ~~and~~ firmware to implement error-control decoding in conjunction with the ~~at least one~~ processor, adapted to process units of data and to detect ~~determine~~ if a unit of data contains at least one uncorrectable error;

a module to run on said ~~at least one~~ processor to determine, based on the pre-determined data poisoning policy, if said ~~at least one~~ uncorrectable error is a data poisoning event, and, if so, to mark ~~as containing a data poisoning event~~ a unit of data containing said ~~at least one~~ uncorrectable error; and

~~at least one~~ an operating system to run on said ~~at least one~~ processor, the operating system ~~to implement a policy~~ to determine, based on the pre-determined data poisoning policy, if a particular data poisoning event is to be acted upon or not, the operating system adapted to detect the ~~presence of a~~ marked unit of data ~~marked as containing a data poisoning event, if the data poisoning event is to be acted upon,~~ and to act ~~upon said presence~~ to mitigate the ~~at least one~~ detected uncorrectable error without always bringing down the operating system upon detection of [[a]] the marked unit of data ~~marked as being bad~~.

15. (Currently Amended) The computer system of Claim 14, further comprising:

a memory coupled to said ~~at least one~~ error control decoding implementation ~~selected from the group consisting of an error-control decoder, software to implement error-control decoding, and firmware to implement error-control decoding~~, wherein the ~~at least one~~ error-control decoding implementation is adapted to process units of data stored in the memory.

16. (Currently Amended) The computer system of Claim [[14]]15, wherein said memory comprises:

a processor cache.

17. (Currently Amended) The computer system of Claim 14, further comprising:

at least one bus coupled to said ~~at least one of an~~ error-control decoding implementation ~~decoder, software to implement error-control decoding, and firmware to implement error-control decoding~~, wherein the ~~at least one of an error-control decoder, software to implement error-control decoding, and firmware to implement~~ error-control decoding implementation is adapted to process units of data passing through the ~~at least one~~ bus.

18. (Original) The computer system of Claim 14, further comprising:

logic adapted to control signaling of information relating to one or more uncorrectable data errors.

19. (Original) The computer system of Claim 18, wherein the logic comprises:

programmable logic.

20. (Currently Amended) The computer system of Claim 18, wherein the information includes a target address corresponding to a unit of data containing ~~at least one~~ the detected uncorrectable error.

21. (Currently Amended) A ~~physical~~ machine-accessible storage medium containing software code that, when read by a computer, causes the computer to perform a method comprising:

pre-determining a software-programmable data poisoning policy to control actions to be taken based on different classes of data poisoning events;

error-checking a unit of data;

if ~~at least one~~ an uncorrectable error is detected in the unit of data, based on the pre-determined data poisoning policy, determining if the ~~at least one~~ detected uncorrectable error is a data poisoning event, and if so, marking the unit of data ~~with an indication that the unit of data contains~~ containing a data poisoning event with a software-visible bit;

determining, based on [[a]] the pre-determined data poisoning policy, if the unit of data containing poisoning event is to be acted upon, and if so, detecting, by an operating system of the computer ~~system~~, the software-visible bit in ~~presence of the indication that~~ the unit of data ~~contains a data poisoning event~~; and

in accordance with the detected software-visible control bit and the pre-determined data poisoning policy, acting, by the[[an]] operating system of the computer~~, upon the presence of the indication~~ to address the presence of ~~erroneous data~~ the uncorrectable error in the unit of data, wherein the operating system is not always brought down ~~upon the presence of the indication~~.

22. (Currently Amended) The ~~physical~~ machine-accessible storage medium of Claim 21, further comprising software code that, when read by a computer, causes the computer to also perform the following:

if the operating system detects the ~~presence of said indication that the unit of data contains a data poisoning event~~ software-visible bit, determining if the unit of data is in user space; and

if the unit of data is in user space, terminating an application running on the computer and removing the unit of data from use by the operating system.

23. (Currently Amended) The ~~physical~~ machine-accessible storage medium of Claim 21, wherein said acting upon the presence of the ~~indication~~ uncorrectable error comprises:

removing the unit of data from use by the operating system.

24. (Currently Amended) A computer system comprising:

~~at least one~~ a processor; and

~~at least one~~ a ~~physical~~ machine-accessible storage medium to be coupled to the ~~at least one~~ processor, the ~~at least one~~ processor to access the ~~at least one physical~~ machine-accessible storage medium and to execute software code stored on the ~~at least one physical~~ machine-accessible storage medium, to cause the computer system to perform a method comprising:

pre-determining a software-programmable data poisoning policy to control actions to be taken based on different classes of data poisoning events;

error-checking a unit of data;

if ~~at least one~~ an uncorrectable error is detected in the unit of data, based on the pre-determined data poisoning policy, determining if the ~~at least one~~ detected uncorrectable error is a data poisoning event, and if so, marking the unit of data ~~with an indication that the unit of data contains~~ containing a data poisoning event with a software-visible bit;

determining, based on [[a]] the pre-determined data poisoning policy, if the unit of data containing poisoning event is to be acted upon, and if so, detecting, by an operating system of the computer system, the software-visible bit in ~~presence of the indication that~~ the unit of data ~~contains a data poisoning event~~; and

in accordance with the detected software-visible control bit and the pre-determined data poisoning policy, acting, by the[[an]] operating system ~~of the computer, upon the presence of the indication~~ to address the presence of ~~erroneous data~~ the uncorrectable error in the unit of data, wherein the operating system is not always brought down ~~upon the presence of the indication~~.

25. (Currently Amended) The computer system of Claim 24, wherein the ~~at least one physical~~ machine-accessible storage medium further comprises software code that, when executed by the ~~at least one~~ processor, causes the computer system to further ~~performs~~ perform:

if the operating system detects the ~~presence of said indication that the unit of data contains a data poisoning event~~ software-visible bit, determining if the unit of data is in user space; and

if the unit of data is in user space, terminating an application running on the computer system and removing the unit of data from use by the operating system.

26. (Currently Amended) The computer system of Claim 24, wherein the ~~at least one physical~~ machine-accessible storage medium further comprises software code that, when executed by the ~~at least one~~ processor, causes the computer system to further ~~performs~~ perform:

removing the unit of data from use by the operating system.

27. (Currently Amended) The computer system of Claim 24, further comprising:

at least one bus ~~coupling~~ to couple the ~~at least one~~ processor with the ~~at least one physical~~ machine-accessible storage medium.